REMARKS

Summary of Telephone Interview

A telephone interview was held with the examiner on 8/17/04 during which the applicant discussed the final office action, particularly paragraph 3 responding to the applicant's remarks traversing the rejections set forth in the first office action. In the final office action, the examiner asserted that certain data structure limitations recited in the claims (e.g., an encrypted message including a client drive ID) are functional as opposed to structural and therefore not given any weight. During the telephone interview the examiner reversed his position, agreed that the data structure limitations recited in the claims provide structural limitations, and agreed to reconsider the applicant's remarks submitted in response to the first office action. Accordingly, the applicant restates below the remarks traversing the examiner's rejections and respectfully requests the examiner address the remarks in the next office action.

Claim Rejections - 35 USC §103

The examiner rejected claims 1-16 under 35 USC §103(a) as unpatentable over Sohne et al (US Patent 6,397,333) in view of Utsumi et al. (US Pub. US 2001/0032088) and in view of Akiyama et al. (US Patent 5,805,699). The applicant respectfully disagrees.

Regarding claim 1, the examiner asserts that Sohne discloses a secure disk drive comprising an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a device ID (col. 3, line 25); a secure drive key; an internal drive ID; and an authenticator for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator responsive to the encrypted message and a client drive key. The applicant respectfully disagrees.

Sohne discloses a copy protection system wherein a device 2 (e.g., a disk drive) comprises a unique identifier (ID) which is communicated to a content provider 1. The content provider 1 combines the device ID with a data set 4 to form a "signed data set" which is transmitted to the device 2. The device 2 authenticates the signed data set by comparing the device ID in the signed data set to the device ID stored in the device 2. If the signed data set is not authenticated, then the data set is not recorded on the device 2. See col. 2, lines 42-57 and col. 4, lines 36-64.

Although the "signed data set" may be considered an encrypted message received by the device 2, the encrypted message does not comprise a device ID for identifying the device that transmitted the encrypted message. In Sohne, the device ID that is included with the encrypted message identifies the device 2 that receives the encrypted message. It does not identify the transmitter of the encrypted message (i.e., the content provider 1).

In contrast, claim 1 recites a secure disk drive that receives an encrypted message from a client disk drive, wherein the encrypted message comprises ciphertext data and a client drive ID identifying the client disk drive (i.e., the transmitter of the encrypted message). The secure disk drive authenticates the transmitter of the encrypted message before allowing the encrypted message to be stored to the disk. In this manner, only encrypted messages received from "trusted" transmitters are stored by the secure disk drive.

The examiner concedes that Sohne does not teach a secure disk drive that receives an encrypted message comprising the ID of the "originator" or transmitter. The examiner asserts that Utsumi discloses a secure disk drive which receives an encrypted message comprising ciphertext data and a client drive ID identifying the client disk drive (transmitter). This interpretation of Utsumi is incorrect. Referring to FIGs. 1-2, Utsumi discloses a license devolution apparatus wherein copyrighted content 13 is copied from a first storage medium 10 to a second storage medium 30. Referring to paragraph 0044, the drive ID of the first storage medium (key 2) is used to decrypt use information 41

(including key 1 used to decrypt the copyrighted content 13) stored in a secure area 12. The use information is then "devolved" to the second storage medium 30. The drive ID 3 of the second storage medium 30 is used to encrypt the use information 42 which is stored in a secure area 32 of the second storage medium 30. Thus, in Utsumi the drive ID (key 2) of the first storage medium 10 is used only to encrypt/decrypt use information 41 stored in secure area 12, and the drive ID (key 3) of the second storage medium 30 is used only to encrypt/decrypt use information 42 stored in secure area 32. Utsumi does not disclose or suggest to transfer an encrypted message (the use information) together with the drive ID (key 2) of the first storage medium 10 to the second storage medium 30. Further, nothing in Utsumi would suggest to authenticate the transmitter of the encrypted message by evaluating the drive ID of the transmitter. The rejection should be withdrawn.

The examiner also concedes that Sohne does not teach to generate a client drive key based on a client drive ID and a secure key, and to generate an internal drive key based on the internal drive ID and the secure drive key. The examiner asserts that Akiyama teaches a key generator for generating a client drive key based on the client drive ID and a secure drive key, and to generate an internal drive key based on the internal drive ID and the secure drive key. The applicant respectfully disagrees.

Referring to FIG. 1 and the abstract, Akiyama discloses a software copying system wherein a central site 5 is used to manage licenses for the right to copy software products. A master storage medium 1 comprises a software identifier for identifying a software product, and a target storage medium 3 comprises a storage medium identifier. The two identifiers are transferred to the central site 5 which generates a first signature based on the two identifiers, wherein the first signature is transferred to the target storage medium 3. A signature generating/comparing unit 8 then produces a second signature out of the same identifiers sent to the central site 5 and compares it with the first signature

stored in the target storage medium 3. A data copying unit then copies the software product from the master storage medium 1 to the target storage medium 3 only if the first and second signatures match.

The software copying process disclosed by Akiyama is completely disparate from the secure communication process recited in the claims. Nowhere does Akiyama disclose or suggest for the target storage medium 3 to authenticate the master storage medium 1. Further, nothing in Akiyama would disclose or suggest to generate a client drive key based on a secure drive key and a client drive ID, wherein the client drive key is used to authenticate the transmitter of an encrypted message (the client disk drive). The rejection should be withdrawn.

The examiner further concedes that Sohne does not teach to transmit a reply from a secure disk drive to a client disk drive, wherein the reply comprises a message authentication code generated using a secure drive key and an internal drive ID. The examiner asserts that a reply comprising a message authentication code is well known in the art, and would therefore be obvious to employ a message authentication code as recited in the claim. The examiner asserts that Akiyama provides the motivation for using a message authentication code for authentication purposes. However, nothing in Sohne or Akiyama discloses or suggests to implement a secure communication process between disk drives by generating a message authentication code using a secure drive key and an internal drive ID. Since the relied upon prior art does not teach any motivation for the modification recited in the claims, the rejection should be withdrawn.

The rejection of the remaining claims should be withdrawn for the reasons set forth above.

CONCLUSION

The above amendments to the specification do not add new matter or raise new issues; the applicant respectfully requests the amendments be entered. In view of the above remarks, the rejections under 35 USC §103 should be withdrawn. In particular, nothing in the relied upon prior art discloses or suggests to implement a secure communication process between disk drives by authenticating the transmitter of an encrypted message based on the transmitter's drive ID. Further, nothing in the relied upon prior art discloses or suggests to generate a message authentication code sent as a reply, wherein the message authentication code is generated using a secure drive key and an internal drive ID. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 8/18/04 By: _____

Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

8/18/04 Howard H. Sheerin
(Date) (Print Name)

_____
(Signature)